UNIVERSITÀ DI TRENTO

Dipartimento di Matematica

DOTTORATO

PhD OPENING 2022

February 7th, 2022 at 9.30

The event will take place online through the ZOOM platform
To get the access codes please contact the secretary office

PhD Program in Mathematics

9.30
Welcome
Valter Moretti (PhD Coordinator)

9.45
Federico Pintore
Dipartimento di Matematica
Università degli Studi di Bari "Aldo Moro"

The re-branding of elliptic-curve cryptography

Abstract: Elliptic curves over finite fields have played a pivotal role in public-key cryptography, both for security and efficiency reasons. However, the possible construction of quantum computers threatens the security of commonly-deployed elliptic-curve cryptosystems. Recently, there have been different proposals to newly exploit elliptic curves for the construction of cryptographic schemes supposed to resist even quantum attacks. Assessing the security of such new schemes and improving their efficiency have put under the spotlight some beautiful maths relative to isogeny graphs, algebraic number theory and quaternion algebras, for which several problems still remain open.

10.45
Virtual Coffee Break

11:00
XXXVII cycle PhD Students Presentation

11:45
PhD talks mathematics: **Alberto Franceschini** and **Sara Sottile**

Information
phd.maths@unitn.it
www.unitn.it/en/drmath